Annexure – A

MATHEMATICS CURRICULUM AND SYLLABUS

For B.Tech. Courses

As per National Education Policy (NEP) 2020 Guidelines

(Applicable from 2024 onwards)

Department of Mathematics

NATIONAL INSTITUTE OF TECHNOLOGY MANIPUR

Langol Road, Lamphelpat, Imphal, Manipur - 795004

A. List of Mathematics Courses for B. Tech. :

Sl. No.	Course Code	Course Name	L	T	P	Credits
1.	MA 1101	Engineering Mathematics-I	3	0	0	3
2.	MA 1201	Engineering Mathematics-II	3	0	0	3
3.	MA 2301	Engineering Mathematics-III	3	0	0	3
4.	MA 2401	Probability and Random Processes	3	0	0	3
5.	MA 2402	Numerical Methods	3	0	0	3
6.	MA 3501	Optimization Techniques	3	0	0	3

B. List of Mathematics Department Open Elective Courses:

Sl. No.	Course Code	Course Name	L	T	P	Credits
1.	MA 4751	Abstract Algebra and Field Theory	3	0	0	3
2.	MA 4851	Introduction to Cryptography	3	0	0	3

Engineering Mathematics - I (MA 1101)

Course Code: MA 1101	Open Elective Course: (Y/N)	Departmental Core Course: (Y/N)	Departmental Elective Course: (Y/N)
	N	Y	N
Type of Course	Theory Course		
Course Title & Code	Engineering Mathematics - I (MA 1101)		
Course Objectives	• To introduce the fundamental concepts of linear algebra including systems of linear equations, vector spaces, subspaces, linear independence, and matrix operations. • To develop the understanding of eigenvalues, eigenvectors, diagonalization of matrices, and inner product spaces with applications to orthogonalization and linear transformations. • To build foundational knowledge in real analysis through the study of convergence of sequences and series of real numbers. • To provide a rigorous understanding of continuity, differentiability, and integration of real-valued functions, along with applications of integral calculus to problems in geometry.		

Course Outcomes		**Cognitive Levels**
CO1	Solve systems of linear equations and analyze properties of vector spaces, subspaces, rank, nullity, and eigenvalues/eigenvectors.	Knowledge/Analysis (Level-I /Level-IV)
CO2	Apply matrix diagonalization, inner product spaces, Gram-Schmidt orthogonalization, and linear transformations over real and complex fields.	Comprehension/ Application (Level-II/Level-III)
CO3	Examine the convergence behavior of sequences and series of real numbers through formal definitions and standard tests.	Application/ Analysis (Level-III /Level-IV)
CO4	Analyze continuity, differentiability, Taylor's theorem, power series, and Riemann integration for real-valued functions.	Application/ Evaluation (Level-III /Level-VI)
CO5	To compute length, area, volume, and surface area of revolution using the fundamental theorem of calculus and improper integrals.	Application/Evaluation (Level-III/Level-VI)

Semester	**I**			**Summer**	
Contact Hours	**Lecture**	**Tutorial**	**Practical**	**Credits**	**Total Teaching Hours**
	3	0	0	3	36
Prerequisite course codes with course names	NIL				

Text Books		
1.	Title	Linear Algebra: A Modern Introduction
	Author	D. Poole
	Publisher	Brooks/Cole
	Edition	3rd Edition
2.	Title	Calculus and Analytic Geometry
	Author	G. B. Thomas, Jr. and R. L. Finney
	Publisher	Pearson Education India
	Edition	9th Edition
3.	Title	Introduction to Real Analysis
	Author	R. G. Bartle and D. R. Sherbert
	Publisher	Wiley India
	Edition	4th Edition, 2014
Reference Books		
1.	Title	Linear Algebra and Its Applications

K. Somasundaram S. Surendra Sunil Pandey

	Author	G. Strang	
	Publisher	Brooks/Cole India	
	Edition	4th Edition	
2.	Title	Linear Algebra	
	Author	K. Hoffman and R. Kunze	
	Publisher	Prentice Hall India	
	Edition	2nd Edition	
3.	Title	A Course in Calculus and Real Analysis	
	Author	S. R. Ghorpade and B. V. Limaye	
	Publisher	Springer India	
	Edition	2nd Edition	
Course Contents	**UNIT I**: Systems of linear equations and their solutions, vector space R^n and its subspaces, spanning set and linear independence, matrices, inverse and determinant, range space and rank, null space and nullity, eigenvalues and eigenvectors.		**10**
	UNIT II: Diagonalization of matrices, similarity, inner product, Gram-Schmidt process, vector spaces (over the field of real and complex numbers), linear transformations.		**8**
	UNIT III: Convergence of sequences and series of real numbers		**8**
	UNIT IV Continuity of functions, differentiability, Rolle's theorem, mean value theorem, Taylor's theorem, power series, Riemann integration, fundamental theorem of calculus, improper integrals, application to length, area, volume, and surface area of revolution.		**10**
Course Assessment	Total Marks=100 Continuous Evaluation 20% Mid Semester 30% End Semester 50%		

Engineering Mathematics - II (MA 1201)

Course Code: MA 1201	Open Elective Course: (Y/N)	Departmental Core Course: (Y/N)	Departmental Elective Course: (Y/N)
	N	Y	N
Type of Course	Theory Course		
Course Title & Code	Engineering Mathematics - II (MA 1201)		
Course Objectives	• To study vector functions, continuity, differentiability, partial derivatives, directional derivatives, gradient, and their applications in geometry and physics. • To analyze maxima and minima, multiple integrals, vector fields, and fundamental integral theorems. • To understand ordinary differential equations, their solutions, and applications. • To explore series solutions, special functions, and system stability.		

Course Outcomes		**Cognitive Levels**
CO1	To analyze vector functions, their continuity, differentiability, and directional derivatives.	Knowledge/ Analysis (Level-I/ Level-IV)
CO2	To apply techniques of multivariable optimization and multiple integration; and to interpret vector fields using fundamental theorems.	Comprehension/ Application / Evaluation (Level-II/Level-III/Level-VI)
CO3	To analyze ordinary differential equations, solution methods, and applications.	Application/Analysis/Evaluation (Level-III/Level-IV/Level-VI)
CO4	To analyze series solutions, special functions, and system stability.	Application/Analysis (Level-III/Level-IV)

Semester	**II**			**Winter**	
Contact Hours	**Lecture**	**Tutorial**	**Practical**	**Credits**	**Total Teaching Hours**
	3	0	0	3	36
Prerequisite course codes with course names	Engineering Mathematics-I (MA 1101)				

Text Books		
1.	Title	Calculus and Analytic Geometry
	Author	G. B. Thomas (Jr.) and R. L. Finney
	Publisher	Pearson Education India
	Edition	9th Edition
2.	Title	Differential Equations
	Author	S. L. Ross
	Publisher	Wiley India
	Edition	3rd Edition
Reference Books		
1.	Title	Calculus-Vol.2
	Author	T. M. Apostol
	Publisher	Wiley India
	Edition	2nd Edition
2.	Title	Elementary Differential Equations and Boundary Value Problems,
	Author	W. E. Boyce and R. C. DiPrima
	Publisher	Wiley India
	Edition	9th Edition
3.	Title	An Introduction to Ordinary Differential Equations
	Author	E. A. Coddington
	Publisher	Prentice Hall India
	Edition	
4.	Title	Ordinary Differential Equations

	Author	E. L. Ince	
	Publisher	Dover Publications	
	Edition		
Course Contents	**UNIT I**: Vector functions of one variable - continuity and differentiability; functions of several variables - continuity, partial derivatives, directional derivatives, gradient, differentiability, chain rule, tangent planes and normal, maxima and minima, Lagrange multiplier method;		**10**
	UNIT II: Repeated and multiple integrals with applications to volume, surface area, moments of inertia, change of variables; vector fields, line and surface integrals; Green's, Gauss and Stokes theorems and their applications.		**8**
	UNIT III: First-order ordinary differential equations - exact differential equations, integrating factors, Bernoulli equations, existence and uniqueness theorem, applications; higher-order linear differential equations - solutions of homogeneous and nonhomogeneous equations, method of variation of parameters, operator method.		**10**
	UNIT IV Series solutions of linear differential equations, Legendre equation and Legendre polynomials, Bessel equation and Bessel functions of first and second kinds; systems of first-order equations, phase plane, critical points, stability.		**8**
Course Assessment	Total Marks=100 Continuous Evaluation 20% Mid Semester 30% End Semester 50%		

Engineering Mathematics - III (MA 2301)

Course Code: MA 2301	Open Elective Course: (Y/N)	Departmental Core Course: (Y/N)	Departmental Elective Course: (Y/N)
	N	Y	N
Type of Course	Theory Course		
Course Title & Code	Engineering Mathematics - III (MA 2301)		
Course Objectives	• To introduce the fundamental properties of complex numbers and the foundational concepts of complex functions, including limits, continuity, and differentiability. • To explore complex integration using anti-derivatives and contour integrals, and apply key results such as Cauchy-Goursat Theorem and Cauchy's Integral Formula, Morera's Theorem, Liouville's Theorem, the Fundamental Theorem of Algebra, and the Maximum Modulus Principle. • To explore techniques for solving first-order partial differential equations using methods such as the method of characteristics, and to classify and solve second-order equations like the wave equation, heat conduction equation, and Laplace's equation using the method of separation of variables. • To apply Laplace and Fourier transform techniques to solve ordinary and partial differential equations arising in mathematical and physical contexts.		

Course Outcomes		**Cognitive Levels**
CO1	To analyze complex functions, limits, continuity, differentiation, and analytic properties.	Knowledge/ Comprehension/Analysis (Level-I/ Level-II/ Level-IV)
CO2	To apply contour integrals, Cauchy's theorems, and fundamental results in complex analysis.	Application/Analysis (Level-III/ Level-IV)
CO3	To perform series expansions, study singularities, and use residue theorem in applications.	Application (Level-III)
CO4	To formulate and solve first-order and second-order partial differential equations using methods such as characteristics and separation of variables, and to analyze initial and boundary value problems.	Application/Analysis (Level-III/ Level-IV)
CO5	To evaluate PDEs using separation of variables, Laplace, and Fourier transform methods.	Application/Evaluation (Level-III/Level-VI)

Semester	**III**		**Summer**		
Contact Hours	**Lecture**	**Tutorial**	**Practical**	**Credits**	**Total Teaching Hours**
	3	0	0	3	36
Prerequisite course codes with course names	Engineering Mathematics - II (MA 1201)				

Text Books		
1.	Title	Complex Variables and Applications
	Author	J. W. Brown and R. V. Churchill
	Publisher	McGraw Hill
	Edition	7th Edition
2.	Title	Elements of Partial Differential Equations
	Author	I. N. Sneddon
	Publisher	McGraw Hill
	Edition	
3.	Title	Differential Equations
	Author	S. L. Ross
	Publisher	Wiley India
	Edition	3rd Edition

4.	Title	Partial Differential Equations: An Introductory Treatment with Applications	
	Author	K.S. Bhamra	
	Publisher	PHI Learning Pvt. Ltd..	
	Edition		
Reference Books			
1.	Title	Visual Complex Analysis	
	Author	T. Needham	
	Publisher	Oxford University Press	
	Edition		
2.	Title	Complex Analysis for Mathematics and Engineering	
	Author	J. H. Mathews and R. W. Howell	
	Publisher	Narosa	
	Edition	3rd Edition	
3	Title	Partial differential equations for scientists and engineers	
	Author	Farlow, Stanley J.	
	Publisher	Dover Publications	
	Edition		
4	Title	Partial differential equations	
	Author	Prasad, Phoolan, and Renuka Ravindran	
	Publisher	New Age International	
	Edition	3rd Edition	
Course Contents	**UNIT I**: Complex numbers and elementary properties. Complex functions - limits, continuity, and differentiation. Cauchy-Riemann equations. Analytic and harmonic functions. Elementary functions. Anti-derivatives and path (contour) integrals. Cauchy-Goursat Theorem. Cauchy's integral formula, Morera's Theorem. Liouville's Theorem, Fundamental Theorem of Algebra, and Maximum Modulus Principle.		**10**
	UNIT II: Taylor series. Power series. Singularities and Laurent series. Cauchy's Residue Theorem and applications. Möbius transformations.		**8**
	UNIT III: First-order partial differential equations; solutions of linear and nonlinear first-order PDEs; classification of second-order PDEs; method of characteristics; boundary and initial value problems (Dirichlet and Neumann type) involving the wave equation, heat conduction equation, Laplace's equations, and solutions by the method of separation of variables (Cartesian coordinates); initial boundary value problems in non-rectangular coordinates.		**10**
	UNIT IV: Laplace and inverse Laplace transforms; properties, convolutions; solutions of ODE and PDE by Laplace transform; Fourier series, Fourier integrals; Fourier transforms, sine, and cosine transforms; solution of PDE by Fourier transform.		**8**
Course Assessment	Total Marks=100 Continuous Evaluation 20% Mid Semester 30% End Semester 50%		

Probability and Random Processes (MA 2401)

Course Code: MA 2401	Open Elective Course: (Y/N)	Departmental Core Course: (Y/N)	Departmental Elective Course: (Y/N)
	N	Y	N
Type of Course	Theory Course		
Course Title & Code	Probability and Random Processes (MA 2401)		
Course Objectives	• To understand the foundational concepts of probability theory, including axiomatic probability, independence, conditional probability, random variables, and their distributions. • To study expectations, moments, moment generating functions, characteristic functions, and analyze standard univariate and multivariate probability distributions. • To explore convergence of random variables, including modes of convergence, laws of large numbers, and central limit theorems. • To understand the fundamental concepts of random processes, with emphasis on discrete-time and continuous-time Markov chains, Poisson processes, and their long-term behavior.		

Course Outcomes		**Cognitive Levels**
CO1	To analyze the foundational principles of probability theory, including independence, conditional probability, and random variables.	Knowledge/Analysis (Level-I/Level-IV)
CO2	To apply standard probability distributions, compute expectations, moments, and utilize generating and characteristic functions.	Knowledge/Application (Level-I/Level-III)
CO3	To evaluate modes of convergence of random variables and apply the laws of large numbers and central limit theorems.	Knowledge/Analysis (Level-I/Level-IV)
CO4	To assess and classify random processes, including discrete-time and continuous-time Markov chains and Poisson processes.	Comprehension/Evaluation (Level-II/Level-VI)

Semester	**IV**			**Winter**
Contact Hours	**Lecture**	**Tutorial**	**Practical**	**Credits**	**Total Teaching Hours**
	3	0	0	3	36
Prerequisite course codes with course names	NIL				

Text Books		
1.	Title	Introduction to Probability Theory
	Author	P. G. Hoel, S. C. Port and C. J. Stone
	Publisher	Universal Book Stall
	Edition	
2.	Title	Stochastic Processes
	Author	J. Medhi
	Publisher	New Age International
	Edition	3rd Edition
3.	Title	A First Course in Probability
	Author	S. Ross
	Publisher	Pearson Education India
	Edition	6th Edition
Reference Books		
1.	Title	Probability and Random Processes
	Author	G.R. Grimmett and D. R. Stirzaker
	Publisher	Oxford University Press

	Edition	4th Edition	
2.	Title	An Introduction to Probability Theory and its Applications	
	Author	W. Feller	
	Publisher	Wiley	
	Edition	3rd Edition	
3.	Title	Probability and Statistics with Reliability, Queuing, and Computer Science Applications	
	Author	K.S. Trivedi	
	Publisher	Wiley India	
	Edition	2nd Edition	
4.	Title	Stochastic Processes	
	Author	S. M. Ross	
	Publisher	Wiley	
	Edition	2nd Edition	
5.	Title	Introduction to Probability	
	Author	C. M. Grinstead and J. L. Snell	
	Publisher	Universities Press India	
	Edition	2nd Edition	
Course Contents	**UNIT I**: Axiomatic construction of the theory of probability, independence, conditional probability, and basic formulae, random variables, probability distributions, functions of random variables.		**10**
	UNIT II: Standard univariate discrete and continuous distributions and their properties, mathematical expectations, moments, moment generating function, characteristic functions.		**8**
	UNIT III: Random vectors, multivariate distributions, marginal and conditional distributions, conditional expectations. Modes of convergence of sequences of random variables, laws of large numbers, central limit theorems.		**9**
	UNIT IV: Definition and classification of random processes, discrete-time Markov chains, classification of states, limiting and stationary distributions, Poisson process, continuous-time Markov chains.		**9**
Course Assessment	Total Marks=100 Continuous Evaluation 20% Mid Semester 30% End Semester 50%		

Numerical Methods (MA 2402)

Course Code: MA 2402	Open Elective Course: (Y/N)	Departmental Core Course: (Y/N)	Departmental Elective Course: (Y/N)
	N	Y	N
Type of Course	Theory Course		
Course Title & Code	Numerical Methods (MA 2402)		
Course Objectives	• To understand error analysis and solve nonlinear equations using iterative methods. • To solve systems of linear equations using direct and iterative methods. • To apply various interpolation techniques for estimating values. • To perform numerical differentiation and integration using standard rules. • To solve ordinary differential equations using numerical methods.		

Course Outcomes		**Cognitive Levels**
CO1	Analyze and estimate errors in numerical computations, and obtain numerical solutions of algebraic and transcendental equations.	Knowledge/Application/Analysis(Level-I/Level-III/Level-IV)
CO2	Solve systems of linear equations numerically and assess the accuracy of the solutions.	Application/Evaluation (Level-III/Level-VI)
CO3	Apply appropriate interpolation and extrapolation techniques to estimate unknown values.	Knowledge/Comprehension (Level-I/Level-II)
CO4	Implement numerical methods for differentiation and integration.	Application/ Analysis (Level-III/Level-IV)
CO5	Solve initial and boundary value problems in ordinary differential equations using suitable numerical approaches.	Comprehension/Application (Level-II/Level-III)

Semester	**IV**			**Winter**	
Contact Hours	**Lecture**	**Tutorial**	**Practical**	**Credits**	**Total Teaching Hours**
	3	0	0	3	36
Prerequisite course codes with course names	Engineering Mathematics - II (MA 1201)				

Text Books		
1.	Title	Numerical Methods for Engineers and Scientists
	Author	Jain, Iyengar and Jain
	Publisher	Wiley Eastern
	Edition	8th Edition
2.	Title	Numerical Analysis
	Author	Richard L Burden, J Douglas Faires
	Publisher	Brooks/Cole, Cengage Learning
	Edition	9th Edition
3.	Title	An Introduction to Numerical Analysis
	Author	Atkinson, Kendall E
	Publisher	John wiley & sons
	Edition	2nd Edition
Reference Books		
1.	Title	Elementary Numerical Analysis – An Algorithmic Approach

	Author	S. D. Conte and Carl de Boor	
	Publisher	McGraw Hill	
	Edition	3rd Edition	
2.	Title	Applied Numerical Analysis	
	Author	Gerald and Wheatley	
	Publisher	Addison – Wesley	
	Edition	7th Edition	
Course Contents	**UNIT I**: Definition and source of errors, propagation of errors, solutions of algebraic and transcendental equations by bisection method, iteration method, Secant method, Newton-Raphson method, Solution of Simultaneous linear equations by Gauss Elimination, Gauss-Jacobi and Gauss-Seidal method.		**10**
	UNIT II: Interpolation: Concept of interpolation, difference operators, divided difference interpolation, Newton's forward, backward interpolation, Lagrange's interpolation, Starling and Bessel's interpolation, spline interpolation.		**8**
	UNIT III: Numerical differentiation (1st and 2nd order), Numerical integration (Trapezoidal, Simpson's one-third, Weddle's rule), Gaussian quadrature.		**8**
	UNIT IV: Numerical Solutions of Ordinary differential equations: IVP: Taylor's method, Picard's method, Runge-Kutta's method, Euler's method and Euler's modified method, Predictor-corrector method. BVP: Shooting method, Finite difference method.		**10**
Course Assessment	Total Marks=100 Continuous Evaluation 20% Mid Semester 30% End Semester 50%		

Optimization Techniques (MA 3501)

Course Code: MA 3501	Open Elective Course: (Y/N)	Departmental Core Course: (Y/N)	Departmental Elective Course: (Y/N)
	N	Y	N
Type of Course	Theory Course		
Course Title & Code	Optimization Techniques (MA 3501)		
Course Objectives	• To introduce students to the classification and theoretical foundations of optimization, covering linear, nonlinear, and dynamic programming. • To equip students with knowledge of key optimization methods, including the simplex method, interior-point methods, duality, and sensitivity analysis. • To develop students' ability to formulate and solve optimization problems in various domains such as transportation and engineering. • To enhance students' ability to use numerical and algorithmic techniques for solving optimization problems, including Lagrange multipliers, KKT conditions, and convex optimization.		

Course Outcomes		**Cognitive Levels**
CO1	Students will be able to model and formulate real-world decision problems as mathematical optimization problems.	Knowledge/Analysis (Level-I/Level-IV)
CO2	Students will demonstrate proficiency in solving linear and nonlinear optimization problems using appropriate mathematical and computational techniques.	Application (Level-III)
CO3	Students will analyze and interpret optimization solutions, including sensitivity analysis and duality concepts.	Knowledge/Analysis (Level-I/Level-IV)
CO4	Students will apply optimization models and tools in practical scenarios, particularly in transportation and operations research.	Comprehension/Application (Level-II/Level-III)
CO5	Students will develop the ability to implement optimization algorithms using computational tools and programming languages to solve complex optimization problems efficiently.	Evaluation (Level-VI)

Semester	**V**			**Summer**	
Contact Hours	**Lecture**	**Tutorial**	**Practical**	**Credits**	**Total Teaching Hours**
	3	0	0	3	36
Prerequisite course codes with course names	NIL				

Text Books		
1.	Title	Linear and Nonlinear Programming
	Author	D. G. Luenberger and Y. Ye
	Publisher	Springer India
	Edition	3rd Edition
2.	Title	Mathematical Programming Techniques
	Author	N. S. Kambo
	Publisher	East – West Press
	Edition	

Reference Books		
1.	Title	An Introduction to Optimization
	Author	E. K. P. Chong and S. H. Zak
	Publisher	Wiley India

K. Somaiah S. Surendra Sunil Pandey

	Edition	2nd Edition	
2.	Title	Nonlinear Programming Theory and Algorithms	
	Author	M. S. Bazarra, H. D. Sherali and C. M. Shetty	
	Publisher	Wiley India	
	Edition	3rd Edition	
3.	Title	Linear Programming	
	Author	K. G. Murty	
	Publisher	Wiley	
	Edition		
4.	Title	The Theory of Linear Economic Models	
	Author	D. Gale	
	Publisher	The University of Chicago Press	
	Edition		
Course Contents	**UNIT I**: Classification and general theory of optimization.		**6**
	UNIT II: Linear programming (LP): formulation and geometric ideas, simplex and revised simplex methods, duality and sensitivity, transportation, assignment, and integer programming problems.		**12**
	UNIT III: Nonlinear optimization, method of Lagrange multipliers, Karush-Kuhn-Tucker theory, numerical methods for nonlinear optimization, convex optimization.		**10**
	UNIT IV: Dynamic programming, numerical methods for nonlinear optimization.		**8**
Course Assessment	Total Marks=100 Continuous Evaluation 20% Mid Semester 30% End Semester 50%		

K. Somorjit Singh

Abstract Algebra and Field Theory (MA 4751)

Course Code: MA 4751	Open Elective Course: (Y/N)	Departmental Core Course: (Y/N)	Departmental Elective Course: (Y/N)
	Y	N	N
Type of Course	Theory Course		
Course Title & Code	Abstract Algebra and Field Theory (MA 4751)		
Course Objectives	• To develop a deep understanding of algebraic structures such as groups, rings, and fields. • To introduce the fundamental theorems of group theory, including Sylow theorems and their applications. • To provide insight into the structure of rings, integral domains, and polynomial rings. • To explore linear algebraic systems and field extensions with a focus on finite fields.		

Course Outcomes		**Cognitive Levels**
CO1	Demonstrate an understanding of basic group theory, including group operations, subgroups, and homomorphisms.	Knowledge/Comprehension (Level-I/Level-II)
CO2	Apply the Sylow theorems and classify groups using advanced group-theoretic methods.	Application/Analysis (Level-III/Level-IV)
CO3	Analyze algebraic structures such as rings, ideals, and polynomial rings.	Analysis (Level-IV)
CO4	Understand and apply concepts related to vector spaces, modules, and field extensions including finite fields.	Application/Evaluation (Level-III/Level-VI)

Semester	**VII**			**Summer**	
Contact Hours	**Lecture**	**Tutorial**	**Practical**	**Credits**	**Total Teaching Hours**
	3	0	0	3	36
Prerequisite course codes with course names	NIL				

Text Books		
1.	Title	Basic Abstract Algebra
	Author	P. B. Bhattacharya, S. K. Jain and S. R. Nagpaul
	Publisher	Cambridge University Press
	Edition	2nd Edition
2.	Title	Contemporary Abstract Algebra
	Author	J. A. Gallian
	Publisher	Narosa
	Edition	4th Edition
Reference Books		
1.	Title	Topics in Algebra
	Author	I. N. Herstein
	Publisher	Wiley
	Edition	2nd Edition
2.	Title	A First Course in Abstract Algebra
	Author	J. Fraleigh
	Publisher	Pearson
	Edition	8th Edition
3.	Title	Abstract Algebra
	Author	Paulsen William

	Publisher	Taylor & Francis	
	Edition	3rd Edition	
4.	Title	Abstract Algebra	
	Author	H. Jonathan K., S. Steven and Sundstrom Ted	
	Publisher	CRC Press	
	Edition	2nd Edition	
Course Contents	**UNIT I:** Groups, subgroups, cyclic groups, cosets, Lagrange's theorem. Group homomorphisms, kernels and images, isomorphisms. Normal subgroups, quotient groups. Permutation groups, alternating and symmetric groups.		**10**
	UNIT II: Group actions, orbits and stabilizers, the class equation. Sylow theorems and Sylow subgroups, applications, p-groups and their properties, Solvable groups and nilpotent groups.		**8**
	UNIT III: Rings, subrings, ring homomorphisms. Ideals—prime, maximal, and principal, Quotient rings, Euclidean domains, Principal Ideal Domains (PIDs), Unique Factorization Domains (UFDs), Polynomial rings over fields and integers. Matrix rings and the ring of quaternions.		**10**
	UNIT IV: Vector spaces over fields, linear independence, basis and dimension. Field extensions: algebraic and transcendental elements, degree of extensions. Simple extensions, finite extensions, and construction of finite fields.		**8**
Course Assessment	Total Marks=100 Continuous Evaluation 20% Mid Semester 30% End Semester 50%		

K-Somorjit Sir

Sunil Pandey

Introduction to Cryptography (MA 4851)

Course Code: MA 4851	Open Elective Course: (Y/N)	Departmental Core Course: (Y/N)	Departmental Elective Course: (Y/N)
	Y	N	N
Type of Course	Theory Course		
Course Title & Code	Introduction to Cryptography (MA 4851)		
Course Objectives	• To introduce the fundamental principles of cryptography and cryptanalysis, including classical techniques and modern approaches. • To explore symmetric key cryptographic systems such as DES and AES, and understand methods of cryptanalysis like linear and differential attacks. • To examine number-theoretic foundations such as primality testing, integer factorization, and the discrete logarithm problem as they relate to cryptographic algorithms. • To understand the structure and applications of public-key cryptography, hash functions, key exchange mechanisms, and digital signature schemes.		

Course Outcomes		**Cognitive Levels**
CO1	Explain the core concepts of cryptography, cryptanalysis, and Shannon's theory of secrecy systems.	Knowledge/Comprehension (Level-I/Level-II)
CO2	Analyze and implement symmetric encryption algorithms, including DES and AES, and understand their vulnerabilities.	Analysis (Level-IV)
CO3	Apply number-theoretic algorithms to problems in cryptography such as primality testing, integer factorization, and solving discrete logarithms.	Application (Level-III)
CO4	Design and evaluate public key cryptographic systems including RSA and understand their role in secure communication.	Analysis/Evaluation (Level-IV/Level-VI)
CO5	Describe and implement cryptographic hash functions, key distribution protocols, and digital signature schemes in practical scenarios.	Comprehension/Application (Level-II/Level-III)

Semester	**VIII**			**Winter**	
Contact Hours	**Lecture**	**Tutorial**	**Practical**	**Credits**	**Total Teaching Hours**
	3	0	0	3	36
Prerequisite course codes with course names	NIL				

Text Books		
1.	Title	Cryptography: Theory & Practice
	Author	Douglas R. Stinson
	Publisher	CRC Press
	Edition	2nd Edition
2.	Title	A Course in Number Theory and Cryptography
	Author	N. Koblitz
	Publisher	Springer
	Edition	2nd Edition

Reference Books		
1.	Title	Handbook of Applied Cryptography
	Author	Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone
	Publisher	CRC Press
	Edition	
2.	Title	Introduction to Cryptography

K. Somorjit Singh Sunil Pandey

	Author	Johannes. A. Buchmann	
	Publisher	Springer	
	Edition	2nd Edition	
3.	Title	An Introduction to theory of numbers	
	Author	I. Niven, H.S. Zuckerman, H.L. Montgomery	
	Publisher	Wiley	
	Edition	5th Edition	
Course Contents	**UNIT I:** Introduction to Cryptography and Cryptanalysis, Classical Cryptanalysis Techniques, Shannon's Theory of Secrecy Systems.		**8**
	UNIT II: Block Cipher: Data Encryption Standard, Advanced Encryption Standard, Linear and Differential Cryptanalysis.		**9**
	UNIT III: Primality Tests, Factoring Integers, Discrete Logarithm.		**9**
	UNIT IV: Problem; Public Key Cryptosystem: RSA; Cryptographic Hash Functions; Key Distribution and Key Agreement; Signature Schemes.		**10**
Course Assessment	Total Marks=100 Continuous Evaluation 20% Mid Semester 30% End Semester 50%		

K. Somajit Singh

Sunil Pandey